March 17, 1959 W. F. FRIEDMAN 2,877,565

ELECTRICAL CRYPTOGRAPH

Filed Aug. 11, 1944 4 Sheets-Sheet 4

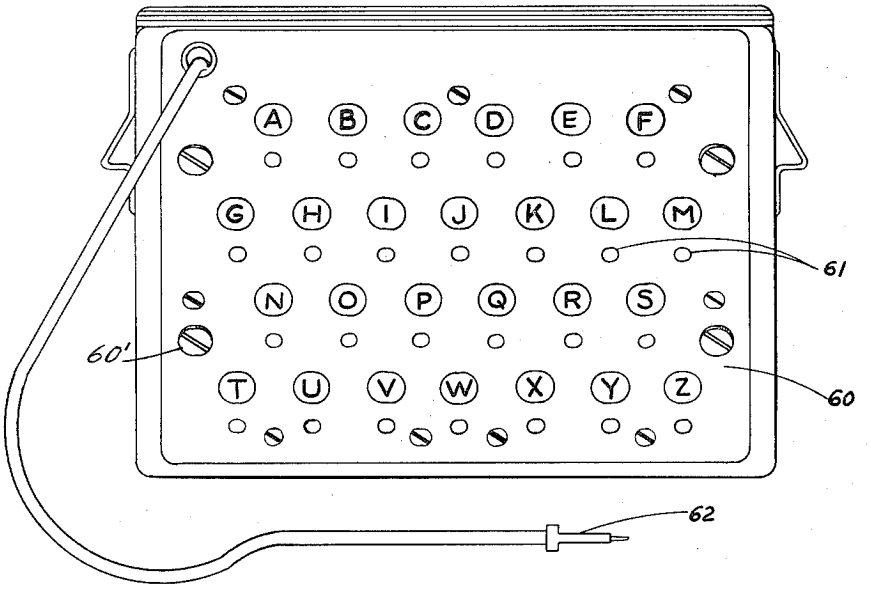

FIGURE 8

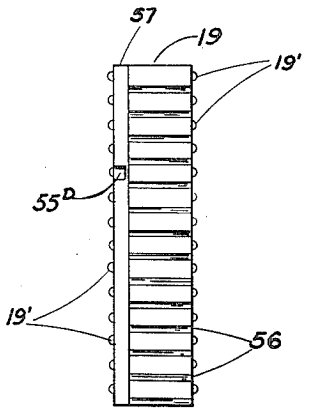

FIGURE 9

WILLIAM F. FRIEDMAN
INVENTOR

William D. Hall.
ATTORNEY

United States Patent Office 2,877,565
Patented Mar. 17, 1959

2,877,565

ELECTRICAL CRYPTOGRAPH

William F. Friedman, Washington, D. C.

Application August 11, 1944, Serial No. 549,086

8 Claims. (Cl. 35—4)

(Granted under Title 35, U. S. Code (1952), sec. 266)

The invention described herein may be manufactured and used by or for the Government for governmental purposes, without the payment to me of any royalty thereon.

This invention relates to a device or machine, which may be used either as a cryptograph for enciphering and deciphering communications, or as an authentograph for testing the authenticity of messages.

The primary object of this invention is to provide a cryptograph or cipher device which is simple in construction and maintenance, but nevertheless affords a high degree of security, is light and readily portable, and can be readily dissassembled and rearranged to vary the cipher keying elements.

Another object of this invention is to provide an authentograph, that is, a device for testing the authenticity of a message or signal, thereby providing means for assuring that such a message or signal originated at an authorized source and is to be considered authentic.

An additional object is to provide a novel keyboard for use with a cryptograph and an authentograph.

Another object is to provide a novel method for the authentication of messages.

Other objects of the invention will become apparent from a reading of the following specification and claims.

In the drawings:

Figure 1 is a top or plan view with the covers closed.

Figure 2 is a top or plan view on an enlarged scale with the keyboard cover and parts of the rotor cover omitted.

Figure 3 is a side elevation with the covers closed.

Figure 4 is a cross section on line 4—4 of Figure 2 with the rotor cover omitted.

Figure 5 is a perspective view of the rotor latch.

Figure 6 is a perspective view of the rotor actuating mechanism.

Figure 7 is a diagram showing schematically the electric circuits and the mechanical operating mechanisms.

Figure 8 is a view of a portion of the device, illustrating a modified keyboard and switching means.

Figure 9 is a view of a rotor such as is used in the device of this invention.

The embodiment of the invention selected from among others for illustration in the drawings and description in the specification is as follows. Referring to Figure 7, the device will be seen, in general, to consist of a source 10 of electricity, connected to a pair of wires 11 and 12 across which are connected a plurality (in this instance, twenty-six) indicators 13A, 13B, 13C, etc. These indicators are illustrated as being electric lamps arranged beneath a keyboard and indicator panel 14 (see Figure 2) and each arranged to illuminate one perforation closed by a transparent cover 15 bearing one letter 16 of the alphabet thereon. Panel 14 is secured in place over a gasket 14' of soft rubber or the like by means of screws as 14''. Across lines 11 and 12 are also connected manually operable switches 17A, 17B, 17C, etc., each in series

with one of the indicators 13A, 13B, etc., arranged for operation by pushbuttons 18 projecting through keyboard 14 in proximity to the covers 15.

Connected to each of the indicators 13A, 13B, etc., is a multicontact electric switch, generally indicated as 19. It comprises a number of relatively juxtaposable and rotatable cryptographic switching wheels or rotors, 19A, 19B, 19C, and 19D, in cascade, each rotor having a plurality of spring input and output contacts 19' thereon (see Figure 9), and a final wheel 19E, which may hereinafter be called the reflecting rotor or reflector, the output contacts of which are connected in pairs, as shown diagrammatically at 20' in Figure 7. Each electrical path, as 20, through the rotor system 19 leads from one stationary contact 20'' through the cryptographic rotors, and back, through 20', to another stationary contact 20''. These paths or circuits 20 are rearranged each time one of the rotors is turned.

In conductor 11 there is a normally-closed electric switch 21. Between one of the indicators, in this case 13E, and multi-contact switch 19, there is a normally-closed electric switch 22. In parallel with wire 11 is wire 11A containing an authenticating switch 23 having an operating handle 24. Wire 11A also contains a normally-open switch 25.

Turning now to Figures 1, 2 and 3 for a disclosure of the mechanical features of the invention, the device is shown as enclosed in a casing 26 to which are hinged or otherwise attached a back cover 27 and a front cover 28.

The front cover, protecting the keyboard, is secured to casing 26 by means of a double hinge 28', 28''. This arrangement permits the cover to fit snugly upon gasket 14', thereby to provide a substantially dust-proof and water-proof closure for the keyboard 14, and yet permits it to lie flat in front of the machine or to be folded therebeneath. The back part of the casing 26, adjacent the rotor assembly, is provided with a lip 26' (see Figure 2). Back cover 27 is adapted to fit over this lip, and has a gasket 27', which provides, upon closure of the back cover, a dust-proof and moisture-proof seal. The front and back covers when closed are secured by means of hasps 23' and 23'', respectively.

In the top of casing 26 there is an opening 29 through which a counter 30 is visible. As is most readily seen in Figure 6, casing 26 has two projecting walls 26A and 26B, which are supported and strengthened by a rod 26C. The cryptographic switching assembly 19 is retained between these walls by a mechanism which will now be described. Wall 26A has an orifice therein through which may be pushed pin 30A having a knurled head 31 (Figure 2) and a latch 32 cooperating with a retaining spring 33. Also pivoted on wall 26A is a spring latch 34 of U-shape, one arm being bent back parallel to the other. The free end 34A of latch 34 is perforated to allow pin 30A to pass through it and bears cam surfaces 35 thereon. Stationary cam 36 has a surface complementary to cam surfaces 35 so that when latch 34 is moved from the substantially horizontal position, in which it is shown in Figures 2, 4, and 6, into the vertical position, in which it is shown in Figure 5, the free end 34A of latch 34 is moved away from wall 26A and compresses the entire rotor-reflector assembly so as to insure good contacts through the spring contacts 19' thereof.

The manually operated means for rotating the cryptographic rotors 19 will next be described. As seen in Figures 1, 2, 3, and 6, casing 26 has a recess 37 in its top into which fits a plunger consisting of fingerpiece 38 having a sliding fit in the recess and a rod 39 upon which the fingerpiece is mounted. Rod 39 causes U-shaped stirrup

40 to turn on its pivots in walls 26A and 26B. On stirrup 40 is a cam 41, which actuates follower 42 fast on shaft 43 of counter 30. Stirrup 40 also has a member 44 to which spring 45 is attached and which carries cam face 46. Detent 47 is pivoted at 48 in walls 26A and 26B and is stressed by spring 49 so that cam 50 engages cam face 46. Spring detents 60 normally hold rotors 19 in their relative positions but allow movement of these rotors under the actuation of pawls 58. Detent teeth 51 are moved in and out of the ratchet depressions in the surface of the rotors 19 upon each movement of stirrup 40, as will be hereinafter further described.

Stirrup 40 carries a pin 52 on which are pivoted a plurality of cam-and-pawl devices, 53A, 53B, 53C, and 53D, which are urged by springs 54 against the rotors (see Figure 9). Device 53B, for example (Figure 6), has a cam 55B and a pawl 58B, and these are adapted to cooperate, respectively, with ratchet depressions 56 of rotor 19A and pawl notch 55D on the rotor 19B.

The operation of this device is as follows: Cover 28 is opened to expose the keyboard 14. If, as frequently happens, limitations of space require, the cover may be folded back beneath the machine. For enciphering or deciphering, handle 24 is operated so that switch 23 is open. That push button 18 which is associated with the desired letter is depressed and the switch controlled thereby is operated. For example (to encipher the letter E), if push button 18 associated with the letter E is depressed, switch 17E (Figure 7) is thereupon closed, and connection is made from battery 10 through line 11, switch 21, line 11B, switch 17E, lamp 13E, and line 12 back to source 10, illuminating lamp 13E. This action also closes connections from battery 10 through lines 11, 11B, through switch 17E, then along line 11C, through switch 22, line 20, thence through rotors 19A, B, C, D and reflector 19E, rotors 19D, C, B, A, to line 20B, lamp 13Z, thence through line 12, back to source 10. Lamps 13E and 13Z are simultaneously lighted, and this indicates that the cipher equivalent of the letter E is Z. To decipher the letter Z, the push button 18 associated with the letter Z is depressed and the circuit is as follows: battery 10, line 11, switch 21, line 11D, switch 17Z, line 20B, through the rotor-reflector assembly, line 20, switch 22, line 11C, lamp 13E, line 12, back to battery 10. Lamp 13E would be illuminated, giving E as the plain-text equivalent of Z. At the same time the lamp 13Z would also be lighted by the closing of switch 17Z and by a circuit which is essentially similar to the one described in connection with the closing of switch 17E. Thus, since rotors 19 connect all the lamps 13A, 13B, etc., and all the switches 17A, 17B, etc., together in pairs, each letter has another corresponding to it.

For rotating the cryptographic rotors 19 and thus varying the connections between the various pairs of lamps 13 and switches 17, the plunger 38 is depressed, stirrup 40 is rotated about its pivots and the members 53A, etc., moved. A pawl 58 will normally ride on a rim 57 of a rotor, and, under these conditions, its associated cam face 55 cannot enter a ratchet depression to step an adjoining rotor notwithstanding the urging of its spring 54. As soon, however, as a pawl falls into a pawl notch 55D it and its cam member move upwardly somewhat and toward the rotors and the latter engages a ratchet depression. Then, on movement of stirrup 40, the rotor in question is stepped. It will be noticed that, in view of the manner in which tang 59 of device 53A underlies device 53B, etc., device 53A cannot move upwardly unless device 53B has so moved. The pawl member of device 53D rises on each operation of stirrup 40, as it drops over shoulder 58' of member 60'. The result is that rotor 19E steps each time the stirrup 40 moves, rotor 19D steps once for each revolution of 19E, 19C steps once for each revolution of 19D, etc.

It is, in other words, the cam face 55 engaged in a peripheral slot 56 and impelled by rotary motion imparted to it by plunger 38—39 which actually serves to step the rotor. The cam face cannot, however, enter into one of the notches until the cooperating pawl enters an auxiliary notch 55D.

Whenever a cam 55 drops into a notch 56, and the movement of the plunger 39 is completed, the corresponding rotor 19 is moved one step. This re-arranges the connections through the rotors and connects different pairs of lamps 13A, etc., together. Counter 30 is moved one numeral because follower 42 is depressed by cam 41 and spring returned. Detent 47 prevents overstepping of the rotors 19 because teeth 51 enter notches in rotors 19.

A detailed description of the operation of the device as an authentograph for insuring the authenticity of a message or a signal will now be given. Assuming that agreement has been previously reached by the two parties concerned as to the wiring of the several rotors and their arrangement in the device, the counter is set to zero, and switch 23 is closed by snapping handle 24. Plunger 39 is then depressed, opening switches 21 and 22 and closing switch 25. This movement moves counter 30 one position forward and also one or more rotors 19 one step. The following circuit is then established: Source 10, line 11, line 11A, closed switch 23, closed switch 25, line 20, thence through the rotor system to whichever lamp happens to be paired with lamp 13E at the moment. Suppose it to be K. The circuit to lamp 13E is at this time open at switch 22 so that lamp E is not illuminated but only the lamp corresponding to its enciphered equivalent, namely K. The letter which is thus paired with 13E becomes an authenticator, which will, of course, be duplicated on a machine similarly set to the same key.

Now suppose that the device is being used to authenticate a plain-language message sent from station A to station B. Having transmitted the message, station A operates its device and finds the authenticating letter to be K, for example. This letter is transmitted as the authentication; station B, operating its device, finds that K is correct and hence is warranted in its belief that the message comes from an authorized source. Upon the next authentication, the letter will be different, since one or more of the rotors will have been advanced on the operation of the plunger 38.

To remove the rotors 19, cover 27 is opened, latch 34 moved from the upright position of Figure 5 to the horizontal position of Figure 6 which allows cam 35 to enter the corresponding groove in stationary cam 36. The compression on the rotor assembly is relieved and, when pin 30 is removed, the rotors can be readily lifted out. To replace the rotors they are merely set in their approximate positions, pin 30 pushed through wall 26A up to its head 31, and latch 34 raised. In the preferred embodiment, the latch, when lowered, extends beyond the end of wall 26A. It thus prevents the closing of the rear cover 27. Since the back cover should normally be closed, the feature mentioned serves to assure that the latch will be up and the roto-reflector assembly properly compressed.

The modification of Figure 8 includes a viewing panel 60, similar in appearance to the viewing panel and keyboard 14 of Figure 2 and similarly secured to the machine by screws, as 60'. In place of push buttons 18, however, viewing panel 60 is provided with contacts only, as 61. These contacts, as shown, consist merely of small circular elements of conducting material all connected by a common return wire 12 to the battery 10. With reference to Figure 7, contacts 61 may be considered as replacing switches 17A, 17E, etc. In place of the push buttons 18, a stylus 62 is provided and this may be considered to be connected to conductor 11 of Figure 7. Encipherment or decipherment is accomplished by making contact between stylus 62 and a desired contact 61 on panel 60.

The above description is in specific terms, but it is to be understood that the invention is not limited to the

precise structures and circuits shown and described. Instead, for the true scope of the invention, reference should be had to the appended claims.

I claim:

1. In a cryptograph having relatively rotatable electric switches arranged in cascade therein, a plunger arranged for manual operation, means associated with said plunger and cooperating upon depression thereof with one of said electric switches for angularly displacing the same, means associated with said plunger and cooperating upon depression thereof with another electric switch for angularly displacing the same after a predetermined angular displacement of said first mentioned switch, and a brake operable by said plunger through a lost-motion connection for preventing more than a desired angular displacement of any switch.

2. The combination with a cryptographic device having a plurality of electrical inputs for the characters to be enciphered, a plurality of electrical outputs for the enciphered equivalents of said characters, a viewing panel including a lamp for each character, a switch associated with each lamp and with a source of current, and a plurality of circuits each including said source, one of said switches, a lamp associated therewith, an input corresponding to the character represented by said lamp, and a lamp corresponding to the output associated with the last mentioned input, whereby the closing of one of said switches will light a lamp representing a character to be enciphered and a lamp representing the enciphered equivalent of said character.

3. In a keyboard for a device of the character described, a switch for each character which may be utilized, a push button extending through the keyboard and adapted upon depression to close a switch, an indicator for each character which may be utilized, each of said indicators being adjacent to one of said push buttons, and means for connecting said indicators and said switches whereby depression of a push button will energize the indicator adjacent thereto and another indicator to show the enciphered character.

4. In a device of the character described utilizing rotors having ratchet depressions in the periphery thereof and a pawl notch, means for stepping the rotors including a stirrup having a limited rotary movement, means for normally holding said stirrup in an inoperative condition, a plurality of cam-and-pawl devices carried by said stirrup, a cam being adapted for cooperation with a ratchet depression of a rotor and a pawl being adapted for cooperation with a pawl notch of another rotor, means for moving said stirrup, means dependent upon said movement

for causing a cam of a cam-and-pawl device to cooperate with a ratchet depression of a rotor, and means for preventing another cam from cooperating with a ratchet depression of another rotor unless the pawl of said last mentioned cam-and-pawl device is also cooperating with a pawl notch.

5. The invention of claim 4, further characterized by means including detent teeth dependent upon movement of said stirrup for moving into engagement with ratchet depressions of the rotors, thereby to prevent overstepping thereof.

6. The invention of claim 4, further characterized by spring detents adapted to rest in the ratchet depressions of the rotors to inhibit the rotation thereof.

7. In a cryptograph including a source of current, a plurality of indicating devices, a normally open switch for each said indicating device, a plurality of permutable electric paths interconnecting said indicating devices in pairs, and means for permuting said paths, two circuits closable by closing each said switch, one including said source of current, the closed said switch, and the said indicating device thereof, and the other including said source of current, the closed said switch, one of said permutable paths, and the interconnected said indicating device.

8. A cryptograph according to claim 7, further characterized by a manually operable switch, and a further switch having two operable positions interposed in a selected one of said other circuits alternatively to connect in its first position the permutable path of said selected circuit to said normally open switch thereof and in its second position to connect said permutable path of said selected circuit to said manually operable switch, means operable by said permutting means for causing said further switch to assume its said second position thereby to close an authenticator circuit including said source of current, said manually operable switch, said further switch, said permutable path of said selected circuit, and the interconnected said indicating device.

References Cited in the file of this patent

UNITED STATES PATENTS

1,096,168	Hebern	May 12, 1914
1,657,411	Scherbius	Jan. 24, 1928
1,683,072	Hebern	Sept. 4, 1928
1,705,641	Korn	Mar. 19, 1929
1,733,886	Korn	Oct. 29, 1929
1,938,028	Korn	Dec. 5, 1933